

# Trusted computing: Bonus or bugbear?

**I**n an age when computer security is uppermost in the minds of most IT professionals, many companies will welcome industry initiatives that promise more secure PCs. An initiative by the Trusted Computing Group (TCG), an alliance that includes Microsoft, Intel, IBM, HP and AMD, and which is the successor to the Trusted Computing Platform Alliance (TCPA), aims to provide just that. Given the nature of Trusted Computing (TC) there is naturally controversy surrounding issues of privacy. This paper presents the views of various experts and participants, but the real debate, of course, will take place at ISSE, so come along and discover just what TC will mean to you and your business!

TC provides a computing platform on which you will not be able to tamper with the application software

In an age when computer security is uppermost in the minds of most IT professionals, many companies will welcome industry initiatives that promise more secure PCs. An initiative by the Trusted Computing Group (TCG), an alliance that includes Microsoft, Intel, IBM, HP and AMD, and which is the successor to the Trusted Computing Platform Alliance (TCPA), aims to provide just that. Given the nature of Trusted Computing (TC) there is naturally controversy surrounding issues of privacy. This paper presents the views of various experts and participants, but the real debate, of course, will take place at ISSE, so come along and discover just what TC will mean to you and your business!

## What is it?

There is increasing recognition that software-only mechanisms are insufficient to protect information. Even the firewall is insufficient as attacks may originate from users inside the company network, or may bypass the firewall completely. The concept behind TC is therefore to provide hardware-based security systems available across a broad range of computing devices with common software interfaces to enable application development and interoperability. In essence, it will provide a remote security solution.

This involves developing both hardware and software standards

which can be implemented by manufacturers. The first two of these, expected in the second half of 2003, are the 'enhanced Trusted Platform Module (TPM) Specification' and a 'new TCG Software Stack (TSS) Specification'.

According to Ross Andersen, of Cambridge University,<sup>1</sup> however, under the TC specification, machines will be more trustworthy from the point of view of software vendors and the content industry, but less trustworthy from the point of view of their owners. Below are two of the main concerns.

## Big Brother

In general, digital objects created using TC systems will remain under the control of their creators, rather than under the control of the person who owns the machine on which they happen to be stored (as at present). So someone who writes a paper that a court decides is defamatory can be compelled to censor it and the software company that wrote the word processor could be ordered to do the deletion if she/he refuses. Given such possibilities, some fear that TC could be used to suppress everything from pornography to writings that criticise political leaders. Naturally this has led to accusations of 'Big Brother' and censorship.

## Lock-in

From a business point of view, there is a fear that software suppliers could make it harder for you to switch to their competitors' products. As a simple example, a software supplier could encrypt all your documents using keys that only they

have access to. This would imply that you could only read them using their word processor. Such blatant lock-in might be prohibited by the competition authorities. There is also a concern that TC applications will work better with other TC applications

## The TCG view

To counter some of these concerns, and particularly the 'lock in' argument, the following statement appears on the TCG website:<sup>2</sup>

TCG will develop and promote open industry standard specifications for trusted computing hardware building blocks and software interfaces across multiple platforms, including PCs, servers, PDAs, and digital phones. This will enable more secure data storage, online business practices, and online commerce transactions while protecting privacy and individual rights.

TCG Benefits include:

- Users will have more secure local data storage and a lower risk of identity theft through both external software attack and physical theft.
- IT organisations will be able to deploy more secure systems and solutions based on open industry standards.



■ Computer, device, and software suppliers will be able to more quickly develop more secure systems and solutions based on open standards.

### The Stanford University view

Tal Garfunkel, Mendel Rosenblum and Dan Boneh of Stanford University also regard TC as a 'positive'. As they state: 'The capabilities trusted computing provides have the potential to radically improve the security and robustness of distributed systems. Unfortunately, the debate over its application to digital rights management has caused its significant other applications to be largely overlooked.'<sup>3</sup>

Their paper looks at technical applications, and the following excerpts outline three of these:

#### Distributed firewalls

Traditionally, firewalls assume that everyone on the 'inside' of the network is trusted, while everyone on the outside is untrusted. However, the increased use of wireless access points, tunnels, VPNs, and dial-ins breaks down the distinction between inside and outside. On a trusted platform a distributed firewall is a significantly more powerful primitive since it can prevent packets that violate the central security policy from ever reaching the network in the first place.

#### Third-party computing

Increasingly, computing resources are being borrowed, leased, or donated by a third party. Examples of this include:

- 1) using donated cycles for massively parallel scientific and mathematical computations by distributed.net, SETI@home, and Folding@home;

- 2) using leased time on commercial computer farms for doing large-scale rendering and animation;
- 3) the emerging field of grid computing that allows heavy users of scientific computing resources to pool and share their computing resources.

The difficulty with this approach to massively parallel computation is trusting the machines doing the computation to:

- 1) produce the correct results
- 2) keep the contents of the computation secret.

Trusted platforms offer an ideal mechanism for solving both problems.

#### Civil liberties protection

Increasingly law enforcement requires the use of network surveillance devices that can potentially infringe on civil liberties. Currently, these devices are certified not to exceed their legal boundaries by inviting a select group of experts to review their design. However, there is no guarantee that the system reviewed by the experts is the one deployed in the field.

Attestation enables us to do precisely that. Building such devices on a trusted platform enables the platform to prove to third parties that the software on the device is the one authorised to execute.

Below are some other applications noted by Andersen:

#### Unlicensed software

TC will make it much harder to run unlicensed software. In the first version of TC, pirate software could be detected and deleted remotely. The mechanisms now proposed are more subtle. TC will protect application software registration

mechanisms, so that unlicensed software will be locked out of the new ecology.

#### Government

Governments will be able to arrange things so that all documents created on civil servants' PCs are classified, and will not be leaked electronically to journalists. Auction sites might insist that you use trusted proxy software for bidding, so that you couldn't bid tactically at the auction.

#### Access control

TC may also be used to implement much stronger access controls to confidential documents. These are already available in a primitive form in Windows Server 2003, under the name 'Enterprise rights management' and people are experimenting with them.

#### Payment systems

TC is also aimed at payment systems. According to Andersen, one of Microsoft's visions is that much of the functionality now built on top of bank cards may move into software once the applications are made tamper-resistant. This leads to a future in which we pay for books that we read, and music we listen to, at the rate of so many pennies per page or per minute.

#### Conclusion

It is clear that TC has a valuable role to play in the drive towards secure computing. It is also clear that there is a great deal of controversy surrounding its introduction. ■

*What do you think?  
Come along to ISSE  
and have your say!*



TC will protect application software registration mechanisms, so that unlicensed software will be locked out of the new ecology

<sup>1</sup> Trusted Computing – Frequently Asked Questions, by Ross Andersen, University of Cambridge Computer Laboratory.

<sup>2</sup> <https://www.trustedcomputing.org/home>

<sup>3</sup> Flexible OS Support and Applications for Trusted Computing, by Tal Garfunkel, Mendel Rosenblum, Dan Boneh, Computer Science Department, Stanford University